СОЦИАЛНОТО ИНЖЕНЕРСТВО – ЗАПЛАХА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ РЕСУРСИ

Ю. Каракънева

Въведение

Независимо от интензивното развитие на информационните и комуникационните технологии, факторите, които са и ще продължават да бъдат определящи по отношение на сигурността на компютърните системи са свързани с традиционните компоненти на тези системи – хардуер, софтуер и интелекта на човека, който участва в целия жизнен цикъл на системите.

Това твърдение е валидно за разпределените системи и за съвременните уеббазирани информационни системи, функциониращи в средата на Интернет или други мрежи.

Известната форма на социалното инженерство, изразяваща се в телефонно обаждане с искане за определена информация или поставяне на спешен проблем, се разви и разпростря в съвременен вариант в глобалното виртуално пространство и е една от главните заплахи за сигурността на информационните активи. Тази заплаха често е пренебрегвана поради факта, че потребителите стават все по-грамотни и квалифицирани и се смята, че са напълно наясно с подходите, използвани от злоумишленици с цел разкриването на ценна информация. Нещо повече, организациите не дооценяват факта, че човешкият фактор продължава да бъде най-слабото място във веригата за сигурност, независимо от инвестициите в сложни и скъпо струващи технологични решения.

Престъпленията във виртуалното пространство (киберпрестъпленията) са основани на съществуващите технологични несъвършенства, но и на психологически тактики [1]. Социалните мрежи и сайтовете на професионалните общности са мишена на злоумишлениците, които извършват злоупотреби, измами и масови манипулации.

Професионалистите в сектора за сигурност би трябвало да са наясно със съвременните техники на социалното инженерство и сериозните заплахи, които този феномен създава в киберпространството. Оценяването на риска и прилагането на адекватни мерки за противодействие са гаранцията за редуцирането на възможностите за успех на тези атаки.

Противодействието е насочено в няколко направления: *превенция, разкриване и коригиране.*

Природа на социалното инженерство

От гледна точка на психологията, социалното инженерство се третира като „изкуството да се накарат хората да изпълняват нашите желания“. Практиката да се получи конфиденциална информация чрез манипулация на човека получи ново развитие с масовото използване на Интернет пространството за обществени и лични цели. Социалният инженер експлоатира естествената склонност на човека да вярва на думите, особено при анонимното присъствие в глобалната информационна среда. Не е необходимо злоумишленикът непременно да е високо квалифициран в технологиите, тъй като използването на слабостите в човешкото поведение е по-лесно от разкриването на пропуските в компютърната и мрежовата сигурност.

В този смисъл някои автори [5, 6] определят социалното инженерство (СИ) като ниско технологично средство, използвано за атаки срещу информационните системи. Нетехническата страна на СИ не изисква финансови средства или знания и умения по компютърни технологии. Използването на психологически подход за подвеждане и манипулиране на потребителите да разкрият чувствителна информация дава забележителни резултати, дори, когато са приложени сериозни технологични средства за сигурност. Същевременно атаките от типа СИ се съчетават с други, технологични атаки – например инсталиране на зловреден софтуер (вируси и червеи) или стартиране на подправени процеси с цел кражба на информация при електронна комуникация.

В частност, социалното инженерство има връзка и с хакерството, извършвано с цел разкриването на пароли или друга информация, която компрометира сигурността на една система. Злоумишлениците очакват да им се предостави възможност от небрежни или недобросъвестни служители или атакуват през мрежата като се опитват да преодолеят контролите и процедурите по сигурността. Експлоатират се връзките между потребителите и изграденото взаимно доверие.

Аспекти на социалното инженерство

Мотивацията на СИ се основава най-често на следните интереси – финансови ползи, лични отношения, отношения в компанията или външен натиск от организация или престъпна група. Най-често обект на атаката са системите, интелектуалната собственост, финансови средства и данни за клиентите.

СИ има класически жизнен цикъл, чиито елементи могат да бъдат разпознати на различен етап и да се реализира адекватна защита. Търсят се пресечните точки на двата цикъла – на атаките на СИ и на политиките за противодействие. Приложена в съответната точка от цикъла на атаката, контролата противодейства и намалява чувствително вероятността за успех.

Цикълът на атаката може да се опише чрез следните елементи: 1. Избор на обект на атаката и събиране на информация за него; 2. Планиране на тактиката и сценариите; 3. Подготовка на средства и инструменти и 4. Създаване на контакт с жертвата и изпълнение на плана. Събирането на информация се извършва най-често от публични източници или от хора от обкръжението на жертвата. Такива данни са, например телефонни номера, лична информация или информация за организационната структура. На основата на наличния информационен ресурс се планират начините за действие – чрез използване на персонален контакт по телефона или в мрежата, чрез имейл, уебсайт или чрез търсене на пробив във физическата сигурност. Създава се връзка с набелязания обект и се привежда в действие планът. Стремежът на атакуващия е в хода на комуникацията да изгради доверие и да разкрие чувствителна информация, която да използва по-късно в интерес на целта си.

Неслучайно се смята, че потребителят следва да бъде включен като *осми слой* в известния OSI модел на архитектурата за обмен на данни между компютри, свързани в мрежа [7].

Хората са податливи на атаките на социалното инженерство защото: са склонни да предоставят информация на висшестоящи; биха искали да помогнат или да се възползват от възможни привилегии или оферти; искат да се реваншират или да изтъкнат своите заслуги; се страхуват да не направят грешки в работата си; се стараят да гласуват доверие на колегите си в общността.

Освен това социалното инженерство се възприема като атака срещу интелигентността на потребителя и той не би си признал за този провал. Немалка роля играе и липсата на компетентност, небрежността и вродената склонност на човека да се противопоставя на правилата и нормативните актове.

Начините, които се използват при атаките от типа СИ се категоризират в две групи – основани на слабостите на човешкото поведение и човешките взаимоотношения и основани на компютърните и мрежовите технологии. Технологичните атаки са насочени към недостатъци на отделните слоеве на мрежовата архитектура и съответните им протоколи. При правилна конфигурация на устройствата в мрежата и приложени контроли, те функционират по точно определен начин. Но хората, участващи в експлоатацията на системите, могат да окажат влияние чрез своето поведение, стимулирано от разнообразни мотиви.

Основните техники, които използва злоумишленикът включват следните разновидности:

- разкриване на информация (пароли, лични данни или данни за системите на организацията) чрез убедително и въздействащо поведение при разговор с потребител или при подслушване на чужди разговори;
- разкриване на информация, съхранявана на компютърна работна станция чрез достъп до потребителско име и парола, когато потребителят не спазва правилата и процедурите за сигурност, например нарушава правилото „чисто бюро" или „чист екран";
- достъп до папката „кошче за боклук" с цел откриване на потенциално ценна изхвърлена информация, спрямо която не се прилагат необходимите мерки за защита;
- изпращане на атрактивни съобщения или оферти, например в анкети или проучвания, чрез които се провокира потребителят да разкрие информация като се предлагат награди или бъдещи ползи;
- използване на бракувано компютърно оборудване (дискове, памети), за което не са приложени мерки за защита на записаната информация и извличане на данни за организация или служители.

При изпълнение на атаката, злоумишленикът влиза в различни ***роли,*** някои от които са:

- *Директна комуникация* с обекта на атаката, при която по подходящ начин изисква от него да разкрие нужната информация. Този начин е най-лесен за изпълнение, но и с най-малки шансове за успех, тъй като се предполага, че грамотният потребител знае, че не трябва да споделя информация.
- *Използване на статута на привилегирован потребител* (мениджър или друг управленски персонал), при което се изисква съобщаването на важни данни, свързани с неотложни задачи. Придобитата информация за софтуера, който се използва, достъпа до сървъра или схемата на конфигуриране на мрежата се прилага по-късно за опит за отдалечен достъп до мрежата на организацията и последващи злоумишлени действия.
- *Представяне като потребител, нуждаещ се от помощ,* например с искане за предоставяне на активен акаунт за достъп до информационната система или забравена парола.
- *Представяне като системен администратор или член на група за техническа поддръжка*, който трябва неотложно да реши системен проблем и за тази цел изисква информация за потребителските данни за достъп.
- *Изпълнение на реверсивна форма на СИ* чрез стимулиране на потребителя да потърси агресора, например чрез оставена в офиса бизнес карта или изпращане на съобщение за проблем, в което се указва контактна информация. Възможно е агресорът да помогне за решаването на системен проблем, за да създаде обстановка на доверие, след което да извърши набелязаната атака.
- *Изпращане на електронни съобщения*, в които са прикрепени файлове с вложени вируси или червеи; изпращане на съобщения, в които се предлага на получателя да ги препрати на колеги или приятели. Специално разработени имейли приканват потребителя да използва фалшиви уебсайтове, които наподобяват легитимни такива.
- *Стимулиране на потребителя да отвори уебсайт*, в който се изисква да се въведе чувствителна информация или лични данни. Използва се всеизвестният факт, че за удобство потребителите използват еднакви или подобни потребителски имена и пароли за различни цели. Освен това тези данни най-често съдържат лична информация като рождени дати в семейството, имена на близки или лични предпочитания, хобита. Тези сайтове се представят като легитимни и провокират потребителят да въведе финансова или лична информация, която по-късно се използва за злоумишлени цели. Същевременно, докато се посещава уебсайт, може да се инсталира зловреден код на компютъра на потребителя, който да послужи за включването на работната станция в зловредна (бот) мрежа.

При привеждането на плана в действие, агресорът използва начини за въздействие върху психиката на обекта. Отклонява се вниманието на жертвата от отговорността, която поема; създава се увереност, че помага да се реши проблем и извършва полезна дейност или извършва услуга, която ще ѝ донесе бъдещи ползи. Залага се на контакта на персонално ниво, свободата на личността и на комуникацията и убеждението, че се взема правилно решение в реално време. Вероятността за успех при атаката се основава на дипломатичен консултативен подход и бърза реакция. Често се използва контакт на основата на предишни полезни връзки. Оказва се влияние върху сетивата и представите на жертвата чрез използване на мултимедийни визуални ефекти или чрез засягане на лични предпочитания.

Противодействие на атаките на СИ

Противодействието срещу атаките на СИ се основава на познаването на заплахите, изучаване на техниките, които злоумишлениците използват и контролните механизми, които могат да бъдат успешно прилагани за защита. Контролите трябва да отговарят на няколко условия: да осигуряват блокирането на различни атаки, които се провеждат едновременно; да не нарушават нормалното функциониране на системата и автоматично да разпознават атаката.

Основни контролни механизми

За гарантиране на сигурността е необходимо ръководството на организацията да разбира ролята си за вземане на решение, дефиниране на изискванията за сигурност и възприемане на мерки, адекватни на рисковете.

За тази цел се разработва стратегия и политика за сигурност, които се изпълняват посредством разработване на правила и процедури за персонала и организацията. Мерките обхващат следните направления:

- *Физическа сигурност*. Установяване на режим на достъп на служителите, посетителите и доставчиците до компютърните помещения и системите. Означаване на категорията за сигурност на помещенията и респективно на статуса на всеки потребител (роля и привилегии) и извършване на проверки за изпълнението на процедурите за сигурност.

Организациите обикновено се насочват към реализиране на логическа среда за сигурност по отношение на компютърните системи и мрежи и често не отделят необходимото внимание на физическата сигурност на информационните активи. Неоторизиран физически достъп до системите или информацията може да компрометира всички елементи на сигурността. Физическата сигурност се простира отвъд вратите и ключалките.

- *Обучение на персонала*. Създаване на тренировъчни програми за обучение на служителите и потребителите и периодично тестване на готовността за реакция при атаки. Гра-

мотните и информирани мениджъри и изпълнители спазват регламентите и режима на достъп и съобщават за съмнително поведение или събитие по отношение на сигурността.

▸ *Изграждане на архитектура за сигурност в организацията*. Създаването на архитектура за сигурност (АС) се реализира още на етапа на проектиране на системите, обслужващи процесите в организацията. Специалните контроли и процедури, въведени в АС гарантират известен автоматизъм при наблюдението и блокирането на атаките и дават възможност администраторите и служителите да се концентрират върху функционалните си задължения и да реагират в реално време.

▸ *Ограничаване на изтичането на данни*. Осъществява се на принципа на редуциране на обема на достъпните чувствителни данни. Например, в уебсайтовете и публичните бази от данни се включва обща информация, която не съдържа имена на служители и други лични данни. Друг начин е ограничаване на достъпа на потребителите до определени сегменти от данни, т.е. разделяне и разпределяне на достъпа чрез дефиниране на роли. При тази ситуация се очаква намаляване на атаките към информационните активи поради факта, че евентуалният обем информация, който може да бъде разкрит не заслужава изразходването на време и средства.

▸ *Изграждане на система за отговор на инциденти*. Политиките и процедурите включват ръководство за действие в случаи на атака. Необходимо е извършване на проверка (автентикация и авторизация) преди извършване на действие. Ако е извършено действие, следва да бъде уведомен администраторът по сигурността, който предприема съответни мерки.

▸ *Създаване на култура в сферата на сигурността*. Важни инициативи в организацията са информиране на служителите и потребителите за рисковете в сигурността, предоставяне на средства за реагиране и насърчаване на комуникацията между персонала по сигурността, мениджърите и служителите. Дългосрочната инвестиция в сектора за сигурност е фактор за гарантиране на защитата на информационните ресурси на организацията.

▸ *Непрекъснат контрол върху механизмите за сигурност*. В рамките на политиката за сигурност се извършва преглед на въведените мерки и средства и дали те отговарят на променената информационна среда. Периодично се извършва одит на инструментите за защита от независими експерти. Един от съвременните подходи за подготовка е провеждането на учения, при които се симулират очакваните атаки и се проверява готовността за отговор и адекватността на процедурите за сигурност. Процесът се подпомага чрез извършване на проверка на публичните домейни на организацията и ценността на информацията, която се публикува.

Нов подход в противодействието на атаките от типа на социалното инженерство е използването на консултантски услуги по сигурността [8]. Консултантските фирми проучват конкретната среда за сигурност в организацията и разработват практическо ръководство за действие.

Особено внимание се отделя на изграждането на т.нар. „човешка защитна стена“. Това означава обучение и тренировки на хората и повишаване на ефективността на действие на човешкия фактор. Подготовката на персонала гарантира определено ниво на разбиране, знания за атаките, противодействие и уведомяване на отговорните лица за потенциални заплахи или съмнителни събития. Потребителите се обучават да не игнорират рисковете и стриктно да изпълняват предвидените процедури за сигурност. Периодично се провежда тестване на служителите във връзка с възникването на нови заплахи. Съставя се ръководство за изграждане на система за превенция чрез обучение за идентифициране на заплахите и защита срещу атаки. Провеждат се компютърно-подпомагани учения с участието на отговорния персонал и преките участници в информационния процес за оценяване на готовността за реагиране на атаки на СИ на двете нива – управленско и потребителско.

Консултантите обобщават резултатите от проучването, извършват оценяване на риска и правят предложение за приоритетите в сигурността и въвеждане на съответни контроли в зависимост от степента на риска. Подобряването на сигурността се основава на прилагане на физически и логически контроли на сигурността на сградите, оборудването, системите и информацията с цел превенция на нерегламентирания достъп до системите, данните и интелектуалната собственост.

Извършва се преглед на физическата сигурност (ФС). Тя е в основата на всеки модел на сигурността. Пробив във ФС компрометира всички останали елементи като хора, системи и информация, които стават потенциално достъпни.

Периметърът на физическата сигурност включва:

▸ персонална сигурност;

▸ обработка на носителите – електронни и хартиени;

▸ откриване и отговор на логически и физически пробиви;

▸ план за физическа сигурност;

▸ физически контрол на достъпа;

▸ физическо наблюдение – камери, достъп и др.;

▸ контрол на средата в критични точки с приложение на информационни технологии – отоплителни, климатични и пожарни системи.

Оценяват се физическите контроли и дали те защитават ефективно офисите и центровете за данни. Дават се препоръки за логическите контроли, които трябва да се приложат, за да се ограничи или избегне достъп до системите и мрежите. Консултантите разработват *изпълнимо ръководство за подобряване на ФС, базирано на реалния риск*.

Физическата сигурност може да бъде скъпа дейност, особено за организации, които работят в условия на финансови рестрикции. Това важи за случаите, когато не е оценен реалният риск от пропуските във физическата среда и не са приоритизирани изискванията. Възможно е да се приложат скъпи решения, които да не са адресирани към най-сериозните рискове.

Като част от прегледа и тестването на физическата сигурност консултантите дефинират приоритетите, базирани на оценката на риска като вземат под внимание уникалните особености на организацията, най-добрите практики на индустрията и регулаторните норми.

Логическите контроли на сигурността може да редуцират влиянието на пропуските във физическата сигурност. Двете направления трябва да се съчетават, за да се постигне приемлива защита на системите, мрежите и интелектуалната собственост.

За да се редуцира вредното влияние на пропуските във ФС, консултантите предлагат начини да се подобри мрежовата организация и контрола на достъпа. Строг логически контрол наред с физическия контрол дава възможност да се създаде модел на сигурността, чрез който да се осигури защита или да се минимизира влиянието на допуснатите недостатъци.

Процесът на противодействие на СИ включва и дейности, свързани с обработката на информацията. Препоръчва се категоризиране и класифициране на информацията и прилагане на специфични контроли за защита срещу случайно разкриване и неоторизиран достъп. Потребителите се обучават да работят с различните категории информация като спазват регламентираните мерки за защита за всяка категория. Разработват се процедури за работа с интелектуалните и фирмените информационни активи и персоналните данни. Разясняват се ролите и отговорностите на служителите, пот-

ребителите и доставчиците, както и предвидените санкции при неизпълнение на нормативните мерки.

Служителите декларират съгласие, че приемат и разбират съдържанието на политиката за сигурност на организацията. Като част от процеса на обучение в сферата на сигурността, организацията провежда периодични тестове на потребителите по въпросите на сигурността, за да определи нивото на разбиране и съгласие с политиките и практиките.

На служителите се предлага да провеждат писмен тест или компютърно-базирано обучение (тренировка), за да се прецени дали притежават знания за политиката за сигурност. Тестовете могат да включват практически упражнения, например контролиране на фишинг сайтове, спам или скам съобщения, като се използва съдържание. Когато се провеждат такива тестове е важно да се осигуряват следните условия:

а) тестовите сървъри и съдържанието да са под контрола на тестващата група;

б) да се ангажират професионални експерти за провеждането на тестовете;

в) потребителите да са подготвени за теста чрез програми за обучение;

г) всички резултати от тестовете да се представят в подходящ формат, с цел защита на правàта на участниците.

Полезните практики, които се включват в правилата за сигурност са насочени към поведението на човека. Подолу са изброени по-съществените правила, които се прилагат:

- отказ за предоставяне на информация на неоторизирани лица;
- следене за настойчиво и съмнително поведение на потребители или клиенти;
- изискване на допълнителна информация от заявителите;
- познаване на категориите информация в организацията и мерките за тяхната защита;
- избягване на споделянето на служебна информация в неформални разговори;
- бдителност за разкриване на фалшива самоличност на клиенти и доставчици;
- обработване и съхраняване на информационните ресурси по предписания от политиките и процедурите за сигурност начин;
- докладване на опълномощените лица при установени заплахи или атаки срещу информационната сигурност.

Заключение

Социалното инженерство е сериозна заплаха за информационните ресурси на организацията и на отделната личност, тъй като се основава на психологическите слабости на човешкия фактор и за привеждането в изпълнение на атаката не е необходима непременно висока техническа квалификация. Атаките се извършват чрез прилагане на различни сценарии, за да се принуди обектът да разкрие информация или да се получи информация без неговото съгласие като се използват слабите места в защитата. Нещо повече, асиметричният характер на тези атаки повишава цената на предотвратяването или елиминирането на вредните последствия.

Ето защо адекватната стратегия за информационна сигурност е критичен компонент за всяка организация или компания и следва да бъде съставна част на общата стратегия за развитие на бизнеса. Негативното влияние на атаките на социалното инженерство може да бъде възпрепятствано чрез разработване на политика за сигурност и на нейна основа прилагане на процедури и мерки, съответстващи на реалния риск. Тези мерки включват:

- изграждане на култура и разбиране за информационна и компютърна сигурност;
- прилагане на контроли за физическа защита и технологични и технически средства за логическа сигурност;
- осигуряване на обучение и подготовка на персонала в областта на сигурността;
- извършване на периодични проверки на ефикасността на съществуващите контролни механизми;
- тестване на готовността на хората за справяне с атаките на СИ.

Използвана литература

1. Каракънева Ю., Киберсигурност, изд. „Авангард Прима“, 2013.
2. Каракънева Ю., Стандарти по киберсигурност, Семинар „Информационна сигурност. Защита от кибератаки“, НБУ, 2013.
3. Каракънева, Ю., Политики в сферата на киберсигурността, Юбилейна международна научна конференция, Нов български университет, 2013.
4. ISO/IEC 27032, “Information Technology – Security Techniques – Guidelines for Cybersecurity”, 2013.
5. Allen, Malcolm, Social Engineering: A Means to Violate a Computer System, SANS Institute InfoSec Reading Room, 2007.
6. Kee, Jared, Social Engineering Manipulating the Source, SANS Institute, InfoSec Reading Room, 2008.
7. Winter C., A Comprehensive Introduction to Computer Networks, 2012.
8. DELL SecureWorks, Prevent Social Engineering From Compromising Your Security, 2014.
9. Collett, Stacy, Four of the newest (and lowest) Social Engineering scams, CSOonline, 2014.

Автор

Юлияна Каракънева – Нов български университет, департамент „Национална и международна сигурност“

75 години навършиха проф. Божимир Давидов, проф. Милан Петров и доц. Цанко Пеевски

Годините минават! Вече повече от две десетилетия сп. “Социална медицина” се опитва да отразява здравно-демографските проблеми, ролята на здравните детерминанти и необходимите мерки за подобряване на общественото здраве. Споменаваме и за някои лични събития, свързани с хората, работили в областта на социалната медицина.

Редколегията поздравява колегите, съратници и приятели на списанието по случай 75-я им рожден ден и дългогодишната им дейност в областта на социалната медицина и организацията на българското здравеопазване.

Пожелаваме им здраве, желание за още работа и плодотворно дълголетие!

Редколегията на списание “Социална медицина”